State of Vermont

Information Security Policy

Date: 11-02-10
Approved by: Tom Pelham
Policy Number:

Contents

1.0 Introduction 3

1.1 Authority 3

1.2 Purpose 3

1.3 Scope 3

2.0 Policy 4

2.1 Introduction 4

2.2 Requirements 4

2.3 Storage of Data 5

3.0 Policy Notification 6

1.0 Introduction

State of Vermont information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised. Logical security tools and techniques are implemented and configured to enable restriction of access to programs, data, and other information resources. Physical access restrictions are implemented and administered to ensure that only authorized individuals have the ability to access or use information resources.

1.1 Authority

The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), "to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government."

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

The unauthorized use, modification, and/or destruction of State of Vermont's information can lead to the loss of valuable information, loss of integrity, possible litigation and other negative impact for the State. The purpose of the is policy is to set forth requirements and guidelines to maintain the confidentiality, integrity, and authenticity of the states information.

1.3 Scope

Security management encompasses all information created or received by State of Vermont Agencies. Security management applies to any activity that involves the access, use, or modification of State of Vermont data and physical properties. The scope or impact is any access, logical or physical, that has the potential to affect State

of Vermont in a negative way. Areas that must be managed include, but are not limited to:

- Physical security
- Logical security
- Granting, moving, and terminating access
- Backup and recovery
- Business continuity
- Network security and monitoring
- Application security (including application acquisition)

2.0 Policy

2.1 Introduction

Access to the State of Vermont's information systems and computing resources will be based on each user's access privileges. Access privileges will be granted on the basis of specific job needs (i.e. a "need to know" basis). Access controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so. All applications will have access controls unless specifically designated as a public access resource.

State of Vermont IT employees are responsible for maintaining secure access to the State of Vermont information systems and computing resources. Access permission levels will be determined by individual departments/agencies as employee supervisors deem appropriate.

2.2 Requirements

To support the Information Security Policy, the following requirements are defined:

1. Terminated employee, contractor, and vendor user accounts to all applications, systems, resources and physical access should be revoked, disabled and terminated immediately following exit.

2. State of Vermont information must be protected from unauthorized disclosure, modification, or destruction. Information about security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of information is not compromised.

3. All hardware and software used by the State of Vermont should be documented and in compliance with all State applicable standards and policies.

4. Documents that contain information that may be sensitive (ie. SS#, HIPAA information, etc.) must be assigned a classification (confidential, private, public) in order to determine the level of sensitivity in which they must be handled.

5. Personnel who have access to sensitive information may require background checks or screenings. Screenings and background checks will be conducted per department/agency and DHR policy.

6. Restricted areas within agencies/departments that house sensitive or critical information systems will at a minimum utilize physical access controls designed to permit access by authorized users only.

7. To maintain the availability, integrity and confidentiality of information, computer and communications equipment should be secured from physical and environmental threats.

8. System capacity requirements should be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

9. Agencies will establish internal procedures for the secure handling and storage of all electronically stored information that is owned or controlled by such agency.

2.3 Storage of Data

Agencies will establish procedures for the secure storage of all electronically stored information that is owned or controlled by such agency/department.

Users with access to State of Vermont customer sensitive information are strictly prohibited from downloading any customer information onto laptops, disk, flash drives, etc. unless the portable device is encrypted. Examples of sensitive information may be a combination of any of the following but not limited to this list:

- Customer name
- Mailing address
- Email address
- Phone number
- Credit card information
- Social Security Number
- Health information

- Banking information

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.